View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Strathclyde Institutional Repository

SFG0019

Written evidence submitted by the University of Strathclyde

Authors:

Department of Electronic & Electrical Engineering:

Dr Greig Paul, Lead Mobile Networks & Security Engineer, Member of DCMS' UK5G Security Group.

Dr James Irvine, Reader & Lead of Mobile Communications Group

School of Government and Public Policy:

Dr Richard Johnson, Lecturer in Government and Public Policy

Anthony Craig, Post-doctoral Research Assistant

Executive Summary

- There are several key technical risks to the UK's 5G and wider mobile network infrastructure. Principally, these cover **espionage, sabotage, and blackmail**[1]. The Committee should ensure they do not overlook the "sabotage" angle – being able to disable the UK's mobile networks would have **devastating impact on the economy, public safety, and wider society**.
- This discussion needs to be about more than purely 5G networks however – the **committee needs to focus on existing 4G networks as well** – 4G and 5G networks are deeply intertwined, and for each site, mobile operators need to deploy 5G from the same vendor as they use on that site for 4G. This plays into the economic arguments made by operators against a ban on Huawei – there is **significant deliberate "vendor lock-in"**, meaning mobile operators did not face a genuine competitive choice between providers – those who had adopted Huawei 4G systems would need to remove and replace those existing 4G systems. Further significant use of Huawei risks further entrenching their equipment, making it even **more costly to remove in future**.
- The interdependency between networks also means that **the option of switching back to a 4G does not exist** should problems arise with the 5G network. Should any capability remain, it is likely to be only a very limited 2G service with practically no data service provision.
- The Government's own advice from **HCSEC around very limited assurance** of Huawei equipment appears to **significantly contradict the assurances Government appears to have**, and the Committee should explore this area further as a matter of priority (details enclosed).
- The UK's decision could well affect the UK's geopolitical position. The UK's **soft power on an international stage may be diminished by the decision**, particularly since much of its soft power is derived from a dedication to democracy, human rights, and civil liberties.

[1] https://foreignpolicy.com/2020/01/31/boris-johnson-britain-knows-its-selling-out-its-national-security-to-huawei/

- The UK's **international standing, particularly with the US, could be impacted** by as few as 3 or 4 **individual senators**, regardless of the quality of relations with the White House[2]. The wider impact of the political sentiment of decisions should therefore be considered.
- From an international prestige and status perspective, even some minor sabotage (i.e. short-term deliberate outage of a UK mobile network) could make the UK look **significantly weakened** on an international stage, and harm the country's reputation as a reliable place to do business.
- Given the Chinese state's past behaviour on offensive cyber action, and Huawei's apparently close links to the Chinese state, there is an elevated potential cyber threat presented.
- From an international relations and diplomacy perspective, a **dependency on another state for critical infrastructure is a weakness** which can be exploited by others.

[2] https://www.spectator.co.uk/article/washington-is-furious-at-boris-s-huawei-bid

What are the risks to the UK's 5G infrastructure? How can these be mitigated?

There are 3 main risks to the UK's 5G infrastructure in the context of this consultation:

1. The **loss of availability (i.e. taking down)** of one or more mobile network, causing knock-on impact to the country and wider economy due to the inability of people to communicate.
2. The **inability to source "end-to-end trustworthy" components** to build our 5G infrastructure for a secure and resilient future.
3. A **targeted attack** carried out to compromise the confidentiality or integrity of messages travelling over the UK's 5G networks (which could exist undetected).

From an international relations perspective, granting the UK's 5G contracts to Huawei creates a potential cyber espionage threat (through backdoors and other design weaknesses in hardware and software) and cyber warfare threat (through control of mobile network infrastructure) to the UK's economic and national security. These concerns arise because of the company's alleged close ties to the Chinese government and China's strong track record of state-sponsored cyber operations against rival countries.

There is documented evidence to suggest that Huawei has very close connections to the Chinese government:

- "Tens of billions of dollars"[3] in **subsidies** from the Chinese **government** helps to explain the company's rapid growth to become a leading supplier of telecoms equipment which has allowed Huawei to undercut competitors like Ericsson or Nokia.
- A study of CVs show **Huawei employees working simultaneously for Chinese military** establishments.[4]
- China's 2017 National Intelligence law obliges Chinese companies to assist the state's intelligence gathering efforts, although Huawei refutes this.[5]

The risk is that Huawei could be required to serve the Chinese state in its cyber espionage operations, which China has previously demonstrated a clear willingness and a capability to engage. Cyber espionage is the most common type of state sponsored cyber operations[6], and academic research shows that out of a total 266 publicly known cyber incidents between rival states from 2000 to 2015, 74 (28%) were initiated by China[7]. According to another database, 140 out of 390 (36%) cyber incidents since 2005 were conducted or sponsored by the Chinese government[8].

---

[3] Chuin-Wei Yap. "State Support Helped Fuel Huawei's Global Rise". 25 Dec 2019. Wall Street Journal. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736

[4] Kathrin Hille. "Huawei CVs show close links with military, study says". 7 July 2019. Financial Times. https://www.ft.com/content/b37f0a9e-a07f-11e9-a282-2df48f366f7d

[5] Yuan Yang. "Is Huawei compelled by Chinese law to help with espionage?". 5 March 2019. Financial Times. https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0

[6] Thomas Rid. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies.* Vol. 35 (1): 5 -32.

[7] Brandon Valeriano and Ryan C Maness. 2015*. Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

[8] "Cyber Operations Tracker", Council on Foreign Relations, https://www.cfr.org/interactive/cyber-operations.

A more serious, yet less likely in the short term, threat is China's use of cyber capabilities against a rival during heightened tensions or conflict, though this is unlikely in the short-term. Given society's growing dependence on computer networks, critical infrastructure and services are vulnerable to computer network attack and sabotage.

Rather than a standalone tactic (given their effects are quickly reversible[9]), **cyber warfare capabilities will likely be employed in any future conflict to disrupt critical services and act as a force multiplier**. If Huawei controls the UK's 5G mobile network, it could theoretically be deliberately **shut off in the run-up to, or during, times of conflict**. This could cause widespread disruption given 5G's future importance to the internet of things and thus the functioning of society.

A far less drastic, but nonetheless serious, use of such capabilities would be to limit the capabilities of the communications networks at key times. Such a tactic would make the UK a less attractive place to do business, and could give a rival a short term advantage.

This problem is not unique to mobile or 5G however, and is relevant to any scenario where digitally-connected critical infrastructure sits under the control of a third-country entity. Clearly much critical infrastructure is inherently not connected to the internet, although with 5G networks this is effectively unavoidable. Where high-risk vendors with state links could be in a position to have the **ability to carry out "power projection" against UK infrastructure**, this should be a clear concern for the Committee.

[9] Eric Gartzke. 2013. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security.* Vol. 38(2): 41-73.

What is the role of government in 5G cyber security?

Government's role in 5G cyber-security is absolutely critical. The DCMS Telecoms Supply Chain Review report (2019) recognised that Government involvement in cyber-security is essential, as a purely **market-driven approach absent close scrutiny does not incentivise investment in security** – commercial operators assume that Government will provide an infinite backstop to defend the nation, and therefore they do not have to bear the cost of this. Not all of the impact of a cyber attack against our telecoms infrastructure would be financial however, and at a time of Covid-19, Government clearly does not wish to be writing blank cheques to enable industry to haphazardly ignore cyber-security in pursuit of the lowest possible prices of equipment, over all other factors.

Our network operators are profitable businesses, and it is only right that they **should bear the cost of making what they provide secure** – were we to be talking about "safety", it would be near unconscionable to suggest that a supplier of a service to every member of the general public would not be responsible for safety.

Cyber-security is a logical extension of the notion of safety – in the same way it is possible to cut costs on building a house by working in a dangerous way, it is possible to cut costs in the design, build and operations of a mobile network by minimising the expenditure on cyber-security, or by **outsourcing key aspects of the network**, putting them outside of the control of staff of the Mobile Network Operator (MNO). It is also possible to cut costs in a mobile network by purchasing from a supplier which offers significantly lower prices, albeit while providing lower levels of technical assurance as to their security.

The role of Government is to scrutinise the capability, competence, and efficacy of their security measures, and **ensure that sufficient security measures are in place to protect the UK's strategic national interests**, so the public have confidence that the networks will be there when they need them the most. The role also includes ensuring that, from a strategic perspective, suitable constraints or regulations are in place to **prevent the "cheapest always wins" approach** – absent external input, generally the cheapest priced solution will be used, to maximise profits. If this is not the intention of Government (as appears to be the case from recent statements in both Houses), the role of Government is **to clarify this clearly to operators** and use **legislative measures** if insufficient powers are available.

To what degree is it possible to exclude Huawei technology from the most sensitive parts of the UK's 5G network while allowing it to supply peripheral components?

This question is a regularly recurring one, and we refer the Committee to a previous response to the Joint Committee on National Security here on this topic, which was dissolved due to the new Parliamentary session before the inquiry completed.[10]

Equipment in mobile networks is inherently inter-connected. One of the challenges previously identified is that **5G networks contain more functionality at the "edge" of the network**, in order to deliver reduced connection latency. This means that some functions which would traditionally be viewed as part of the "core" may end up at the edge of the network, integrated with equipment from high-risk vendors. This means that it is very hard to exclude any one vendor from supplying radio equipment to the network, while preventing them from meaningfully interacting with the core network (noting that in a mobile network, the radios inherently communicate directly with the core network).

A broader question to be asked here is the **extent to which this distinction makes sense**, and the impact that the decision may have. For some of the high-profile use-cases of 5G networks, such as Industrial IoT and Connected/Autonomous Vehicles, there may be **safety critical aspects of the system**, located at the network edge. These would be provided by the peripheral components, which **could be from high risk vendors, absent clarification from Government that this will never be acceptable**. Alternatively, the impact of an outage on the overall system itself may be such that it is critical, by virtue of the consequences of it failing. For this reason, the distinction around peripheral and non-peripheral components is not as clear-cut as the legislation suggests.

In line with NCSC's advice, high risk vendors should not be used to provide systems which are used for safety-critical applications, or for critical national infrastructure. A decision to permit active radio elements of the mobile network would preclude a network from being used for safety-critical or CNI purposes. Given the potential future uses of 5G, this would seem to hold the UK back. Operators are likely to deploy the lowest cost radios, to maximise profits, since they are not in the business of spending money they do not have to.

It is important to also note that Government advice states operators should not use equipment from high risk vendors at special protected sites. Given how mobile operators design and deploy their network in "zones", with **each zone using interoperable equipment from the same vendor**, there are clear practical challenges. If the only constraint placed on operators is around the geographic positioning of high risk vendor equipment in relation to the sensitive site, the Committee should consider the impact of **all access routes to this sensitive site involving passing through areas of radio equipment from high risk vendors**. The measures in place to prevent high risk equipment from **interacting or communicating with low risk vendor equipment** should also be explored further by the Committee – networks are inherently designed to facilitate communication between components, and both **4G and 5G networks feature direct, base station to base station communications** to enable handovers as users move between base stations. **It does not appear that current guidance addresses this major issue**.

[10] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/ensuring-access-to-safe-technology-the-uks-5g-infrastructure-and-national-security/written/105444.html

What credible alternatives are available to Huawei systems?

For radio network equipment itself, there are only 3 widely available vendors – Nokia, Ericsson and Huawei. There are other vendors with much more limited market share, which have little or no footprint in the UK and Europe – these include Samsung, for example, though they are significant in end-user devices like handsets.

There are alternatives to these traditional Tier-1 suppliers, however, which present completely independent supply chain options. The UK mobile network operators have historically not considered these, and prefer to favour the traditional Tier-1 vendors. **These options should be prioritised** by Government as options to **diversify the supply chain**, as well as introduce opportunities for export to our allies.

Members of the Committee should note that the 5G RuralFirst project (based in the Orkney Islands) successfully demonstrated that new, innovative equipment can be used to build mobile networks in some of the most challenging environments possible, and that these work with existing handsets and equipment. Therefore, to some extent, the problem is commercial, rather than technical. **No equipment from high-risk vendors (or indeed any Tier-1 vendors) was used for the radio network in that project.** This proves that there are alternative approaches that can be utilised to build secure mobile networks without relying on the existing limited supply chains.

One challenge the UK (and other countries) face is that mobile operators like to build their network in large zones and **utilise the same vendor's radio equipment throughout that zone**. This is to facilitate the planning and operation of their network in that zone – despite these mobile networks being standardised, **radios from competing vendors are not interoperable in a "plug-and-play" manner**. This raises the cost of switching radio vendor significantly, and results in a very high barrier to entry for innovative players in this space. In 5G RuralFirst, for example, we were able to build a green-field network without having to work around the constraints of an existing "Tier 1" vendor's network management software. Commercial operators are held back by the **lack of inter-vendor interoperability in network standards**, and this is an area the **UK should aim to take leadership of, in the global standards arena**, via the existing DCMS Testbed & Trials funded programs.

There is a challenge around commercial incentives here for the committee to consider – a mobile operator clearly wants to build the lowest cost solution, in order to maximise the potential profit which can be made from the system.

To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?

The UK Government's decision was largely foreseeable in advance, and driven by both commercial and political factors. The UK's mobile operators exerted **significant lobbying influence** over Government during the process – to some extent, the Government's decision came too late for an outright restriction to be issued. Operators had been rolling out 5G in earnest for many months prior to this ruling coming through, having sought clarity and received little beyond a confirmation that the existing guidance (that high-risk vendors could be used in the network, albeit not in the core of the network) would be revised.

Thorsten Benner, director of the Global Public Policy Institute, believes the decision is political due to **fear of retaliation**, citing the Chinese ambassador stating in an interview that exclusion would lead to worsening economic and political relations. He believes that Chinese threats to the UK over economic and political relations worsening were seen as more salient to the UK than US threats.[11] The US was also reported to have provided clear "intelligence information" at the end of 2019, showing "that Huawei cooperates with China's security authorities"[12]. While this is likely true for many businesses around the world, it is important for the committee to remember that this discussion pertains to the **UK's own critical national infrastructure**.

This perhaps becomes clearer when considering that accepting high risk vendors in the 5G network would hinder moving towards OpenRAN and other **interoperability-driven initiatives**, which aim to avoid the lock-in scenario the UK is currently in, with edge 4G and 5G radio equipment needing to be from the same vendor. Failing to move towards interoperable systems **would increase market barriers to entry by existing or new rivals in the future**, further entrenching the problem and increasing the cost of moving to other providers[13].

From a public opinion perspective, the Government **lacks public pressure** against the decision due to **lack of knowledge** about the issue. According to a YouGov survey from April 2019, 34% of British adults opposed the decision to give the 5G contract to Huawei, while only 22% supported it. However, **44% responded 'don't know'**, suggesting a lack of understanding of, and therefore engagement with, this issue by the public.[14]

Unlike the US and Australia, much of the UK's telecommunications infrastructure, including 4G, is provided by Huawei already. An outright ban would mean the UK's mobile networks would need to invest in removing existing 4G Huawei technology, which would be economically and politically costly by delaying the government's pledges of 5G rollout.[15] BT have already announced that replacing existing Huawei infrastructure in order to meet the government's 35% cap policy will cost them £500m over five

---

[11] https://foreignpolicy.com/2020/01/31/boris-johnson-britain-knows-its-selling-out-its-national-security-to-huawei/

[12] Ibid.

[13] Ibid.

[14] YouGov. "Do you support the decision to let Huawei help build the UK 5G network? Plus, converting offices into housing, and the role of the Bank of England results". 24 April 2019. https://yougov.co.uk/opi/surveys/results#/survey/00a12913-6671-11e9-9042-bd2e3c2704ca

[15] Emily Taylor, "Who's Afraid of Huawei? Understanding the 5G Security Concerns". Chatham House. 9 September 2019. https://www.chathamhouse.org/expert/comment/who-s-afraid-huawei-understanding-5g-security-concerns#

years.[16] It is worth noting that **EE is the network operator responsible for delivery of the UK's Emergency Services Network**, and the recent announcement of a 2-year delay to the removal of Huawei equipment from BT's core network[17]. This would suggest that the UK's long-delayed ESN project will continue to incorporate a Huawei core until 2023 at the earliest.

These timescales are also useful, as they demonstrate to the Committee the very real difficulty in reversing this decision going forwards **– BT made the decision to remove Huawei equipment from its network core in 2018**, and said that would be completed by **2020**. Due to the requirement to also reduce Huawei's presence in the radio access network to 35%, BT now says this **original task will take until 2023**. The level of technical confidence that Government feels it has over the integrity and security of the providers of its critical infrastructure must therefore **take into account the timelines that would be involved in removal and replacement to reverse this decision**, were this to prove incorrect. The vendor of edge equipment on the UK's telecoms network cannot be changed overnight – it would be a **multi-year, multi-billion pound project**, at a time where we can least afford to undertake it.

The UK set up the Huawei Cyber Security Evaluation Centre in 2010, under the purview of the National Cyber Security Centre to test Huawei's components for security flaws. HCSEC has not, to date, found security flaws it believe stem from any Chinese Government interference.

Nonetheless, it is critical for the Committee to note several points reported by HCSEC, since the **Government's position** and justification of its decision was heavily **based on the premise that security risks "can be managed" given the restrictions proposed**.[18]

In contrast, the HCSEC's most recent (2019) annual report[19] states

1. HCSEC has consistently stated through its oversight board reports that the board can "provide **only limited assurance** that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK" (emphasis from original report) – if **such little assurance** can be provided for **currently deployed** equipment, the Committee should question why Government is so confident it can manage the security risks its own advisors highlight.

2. HCSEC has highlighted much of Huawei's software "**lacks basic engineering competence**" and "significantly increased risk to UK operators", and that some of their coding practices make the "job of any code auditor exceptionally hard", and could be explained by "developers… **actively working to hide bad coding practice** rather than fix it".

3. HCSEC's board has warned "**it will be difficult to appropriate risk-manage future products**… until the underlying defects in Huawei's software engineering and cyber security processes are remediated…"(emphasis from original report), and that the board "has **not yet seen anything to**

[16] Joe Curtis. "Government's Huawei 5G cap will cost BT £500m". City AM. 30 January 2020. https://www.cityam.com/bt-profit-falls-as-telecoms-giant-blames-regulation-costs/

[17] BT delays removal of Huawei from EE's core network by two years. BBC News. 15th April 2020. https://www.bbc.co.uk/news/technology-52296666

[18] https://www.ft.com/content/5bef8972-405a-11ea-bdb5-169ba7be433d

[19] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

> **give it confidence in Huawei's capacity to successfully complete … its transformation program** that it has proposed as a means of addressing these underlying defects."

These, and many other key points from the report, should be brought to the Committee's attention, since much of **the assurance the Government appears to be basing its decision on does not match with HCSEC's own board's reporting**. These findings are technically very significant, as they highlight the challenges in providing assurance, and perceived likelihood of being able to get this assurance in the future. Assurance which Government is basing its decision on. This makes it seem **doubtful that the Government's approach was based on technical evidence**, at least based on that available from HCSEC.

Professor Steve Tasng, director of the China Institute at SOAS University of London believes the threat comes in from software updates, with "constantly updating code making it harder to maintain complete oversight", and the level of risk being changeable, and therefore no longer manageable a few years down the line.[20]

Terry Dunlap, a former NSA hacker and co-founder on cybersecurity firm ReFirm Labs, sees an economic strategy as a concern here: "They get their foot in the door via the subsidized pricing and then continue to eat away at the incumbent… As a result, the eventual switching costs you would face from a non-subsidized replacement option are huge. Slowly over time more and more pieces of communications gear will be replaced by Huawei gear… Your security is controlled by the vendor, who may or may not choose to fix certain vulnerabilities. I guess that can be said about any vendor — but not all vendors have their government as a business partner."[21]

[20] https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html
[21] https://breakingdefense.com/2020/01/huawei-not-ok-for-uk-intelligence-experts/

How will the UK Government's decision impact the UK's geopolitical position?

From an international influence perspective, the evidence suggests that the UK's geopolitical position would not likely be impacted significantly, as the decision is relatively small compared with the impact of Brexit. The UK's soft power influence may be impacted somewhat, however.

Eric Sayers – senior adjunct fellow at the Center for a New American Security – believes the **UK decision will influence other states'** decisions on Huawei amid American pressure[22]. Michael Rogers, former Congressperson and chair of the House Intelligence Committee and now head of 5G Action Now, believes the **US should now focus on Poland, Germany, and Canada** to prevent them "from polluting their networks"[23].

According to the European Council on Foreign Relations, the UK has a lot of soft power[24], as opposed to traditional military strength, but if the US and Australia were perceived to be less likely to pursue a free trade deal now due to Huawei decision, or use this to improve their negotiating position, and the UK was perceived to "lose" in the negotiations then this could present a negative impact on the UK's prestige in international relations. Early indications indicated that US Vice President Mike Pence said that a Huawei deal could be a "deal-breaker" for a US/UK free trade agreement in February 2020[25].

Although the decision does not directly impact the UK's military capabilities, it could negatively impact UK's geopolitical position by boosting the relative power of China in international politics, by reducing UK's influence through dependence on a foreign state, threatening the western alliance system, and by undermining UKs soft power image.

Huawei has **won more 5G contracts than Nokia or Ericsson** (over 90 contracts with mobile carriers in foreign countries so far)[26], and by giving one of China's largest telecoms company an even greater global market share in 5G supply, the UK's decision may aid China's rising influence in the global economy and boosts its relative power in international politics.

Despite the UK's long-term decline in conventional military capability over the past few decades, it is arguably still a major power in international politics with a nuclear deterrent, permanent seat in the UN security council, and top 10 military spender[27]. The UK is also a leader in cyber capability. 5G doesn't affect these facts. Brexit will reduce UK's influence, but again this is independent of Huawei and 5G. A country's geopolitical influence comes also from its alliances and the 5G issue may threaten the Five Eyes alliance specifically – 3 of the five eyes nations (USA, Australia, New Zealand) have banned Huawei[28], and the UK's alliances are generally essential to presenting a unified and credible deterrent against threats – for example, the NATO alliance.

---

[22] https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html
[23] https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html
[24] https://www.ecfr.eu/article/commentary_the_big_squeeze_british_foreign_policy_after_brexit
[25] https://www.independent.co.uk/news/uk/politics/mike-pence-huawei-5g-boris-johnson-uk-trade-deal-us-brexit-trump-latest-a9324086.html
[26] https://asia.nikkei.com/Business/China-tech/Huawei-claims-over-90-contracts-for-5G-leading-Ericsson
[27] https://www.ecfr.eu/article/commentary_the_big_squeeze_british_foreign_policy_after_brexit
[28] https://www.telegraph.co.uk/politics/2020/03/04/uk-risks-plunging-five-eyes-alliance-crisis/

On the other hand, however, Huawei's access to the UK's mobile networks potentially increases China's political and economic leverage over the UK as well as posing the cyber espionage/warfare threats as explained earlier.

It is worth the Committee considering how the UK's soft power image comes from its dedication to democracy, human rights, and civil liberties[29], and the UK government should consider whether it wants to be seen to be benefitting an authoritarian country with a divergent approach to western ideas of democracy, human rights and civil liberties. The UK came top in the world for soft power in the 2018 and 2015 Portland Group, Comres & Facebook report[30,31]. The Committee should consider the impact on soft power and perceived strength if the UK is seen to not be able to provide and run its own 5G networks, at a time when 5G is increasingly important for nations.

[29] https://www.gov.uk/government/speeches/foreign-office-minister-talks-of-using-soft-power-in-the-interests-of-the-uk

[30] https://comresglobal.com/wp-content/uploads/2015/07/Report_Final-published.pdf

[31] www.portland-communications.com/wp-content/uploads/2015/07/The-Soft-Power-30_press-release.pdf

How will the UK's allies, particularly those in Five Eyes, respond to this decision?

There has been significant press coverage over the how representatives of the US in particular have responded, both ahead of, and in response to, the UK decision.

The US Secretary of State, Mike Pompeo, stated the Five Eyes network is strong, despite Britain's decision [this week] to not exclude Huawei from providing 5G telecom equipment (Feb 2020)[32], and that he was "very confident that our two nations will find a way to work together to resolve this difference"[33]. The US President's acting chief of staff – Mick Mulvaney – told Oxford Union that a "direct and dramatic impact" on intelligence sharing will occur[34].

Former Speaker of the House, Newt Gringrich, called the decision a "major defeat" for the US; Senator Tom Cotton (R): equated the situation with allowing the KGB to build the UK telephone network during the Cold War; Senator Mark Warner (D) said he was "disappointed in UK's decision…the United States remains committed to working with the UK and other key allies to build more diverse and secure telecommunications options that provide competitive alternatives to Huawei"[35]

Senator Ben Sasse (R), a member of the Senate Intelligence Committee, took a very negative view, saying "Here's the sad truth: Our special relationship is less special now that the U.K. has embraced the surveillance state commies at Huawei," and that "The Chinese Communist Party has infected Five Eyes with Huawei, right at a time when the US and UK must be unified in order to meet the global security challenges of China's resurgence."[36]

An anonymous Senate staffer was quoted by the Spectator as saying, "What our British friends need to remember is that it is ultimately the Senate, and not the President, who will decide whether a trade deal passes. A few frustrated Senators have the power to put major blocks on trade legislation."[37] For example, Senator Sasse is from Nebraska; a state that in 2016 had over $12 billion in receipts from livestock sales.[38] A senator upset about 5G decisions may not want a trade deal with a country that will not accept his constituents' beef or chicken.

In letters sent from US Senators to the UK Prime Minister[39], Rubio, Cotton and Cornyn said that:

"Between 1998 and 2019, Huawei received more than $75 billion in subsidies, grants, land licenses, and other forms of financial assistance. Huawei has also routinely undercut its competitors' prices, triggering anti-dumping investigations in the European Union and India. Last year, the Huawei 5G bid in the

[32] https://www.reuters.com/article/us-britain-usa-huawei-pompeo/pompeo-backs-five-eyes-intelligence-sharing-despite-uk-decision-on-huawei-idUSKBN1ZT1IV
[33] https://www.cnbc.com/2020/01/30/pompeo-plays-down-rift-with-britain-over-huawei.html
[34] https://www.telegraph.co.uk/politics/2020/02/19/huawei-decision-will-have-dramatic-impact-us-ability-share-security/
[35] https://www.theguardian.com/politics/live/2020/jan/28/labour-says-government-claim-to-be-reversing-beeching-rail-cuts-meaningless-live-news
[36] https://breakingdefense.com/2020/01/huawei-not-ok-for-uk-intelligence-experts/
[37] https://www.spectator.co.uk/article/washington-is-furious-at-boris-s-huawei-bid
[38] https://agecon.unl.edu/cornhusker-economics/2018/livestock-production-value-economic-impact-nebraska
[39] https://www.rubio.senate.gov/public/index.cfm/2020/1/rubio-cotton-cornyn-urge-members-of-united-kingdom-s-national-security-council-to-reject-huawei-in-5g-infrastructure

Netherlands was 60 percent less expensive than its nearest competitor, a difference which, according to industry experts, does not even cover the cost of parts. No one can compete with a company that has the Chinese government absorbing its losses. Ultimately, allowing Huawei to participate in the United Kingdom's 5G infrastructure undermines the goals of supply chain diversity and providing the best options for the British people."

"The economic arguments in favour of Huawei fall apart when the costs of risk mitigation are included. Managing risk on 5G networks is more difficult than existing 3G and 4G networks, because the software integration between the equipment erodes, if not eliminates, the "core" versus "edge" distinction. Reviewing the code as it is updated is a monumental task. This cost never goes away, because each update will require another round of review. Moreover, there is a human cost to consider. Hiring and training the people to do this means that otherwise talented individuals, at the expense of U.K. taxpayers and consumers, will be working to make Huawei better rather than investing their time and energy in creating a new program, a new company, or new jobs for working towns in Britain."

Elsewhere in the five eyes alliance, Australia banned Chinese vendors from supplying technology to its 5G networks in 2018. As of the 10th of March 2020, Huawei has stated it is not currently trying to reverse this 5G ban, and was "not trying to win that battle anytime soon" [40].

Canada has yet to make a decision, but their military was reported in February 2020 to have told the Canadian Government they believe allowing Huawei a role in their 5G networks would threaten national security[41].

Dr John Hemmings – associate fellow at the Henry Jackson Society and associate professor at a US Department of Defense academic institute – sees diplomatic damage resulting from the UK's decision between the US and Australia, with slightly less damage with Canada and New Zealand, as a result of the UK being perceived to treat this "as a solely Huawei-related problem, rather than a broader China issue"[42].

The UK's allies in Europe have generally taken a broadly similar approach to the UK – the European Commission's "toolbox"[43] have been reported to be a "far cry from a hard ban". The approach being recommended does not single out any country or company, but advises member-state governments to assess risks associated with vendors, taking into account factors such as headquarters location, surveillance rules the company is subject to, and whether it is able to challenge government requests for espionage through "democratic checks and balances". These measures are reported to be "without a doubt, targeted at China and its vendors, Huawei and the smaller rival ZTE"[44].

[40] https://www.gizmodo.com.au/2020/03/huawei-5g-australia/
[41] https://www.bloomberg.com/news/articles/2020-02-10/military-wants-huawei-banned-from-5g-in-canada-globe-says
[42] https://www.telegraph.co.uk/politics/2020/03/04/uk-risks-plunging-five-eyes-alliance-crisis/
[43] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[44] https://www.politico.eu/article/europe-eu-huawei-5g-china-cybersecurity-toolbox-explained/

How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?

In the unlikely event of a land invasion of the UK, then there could be an impact on security and defense capabilities, although it is important to note that the UK's public mobile networks are those being discussed, rather than the dedicated military communications networks. However, when acting internationally, the military uses other communications techniques which are not part of the regular public commercial telecoms networks.

In terms of interoperability, future coalitions – particularly US and UK if not all of NATO – would need a compatible portable system that can be moved/relocated into areas of operation, and it would be important to ensure that these systems were interoperable across the coalition of allies, and not exposed to the kinds of concerns identified here.

How important it is for the UK, separately or with allies, to maintain industrial capability in this field?

It is **incredibly important** that the UK, both separately, as well as with its international allies, **creates capability in this field**. The phrase "creates" is specifically and deliberately used, as the **UK has lost a lot of its historical industrial capability in telecoms**. There are a number of challenges and barriers to this, including around the economics of achieving this:

1. **Addressing the off-shoring and out-sourcing of the operation of our networks**

   There has been a significant drive to **out-source key components** of mobile networks**, including to companies now deemed to be high-risk vendors**. This creates the risk of a significant capability gap, especially where skilled personnel are transferred out of UK companies to foreign companies. The committee should look at the scenario where, in **December 2018, O2's network was unavailable for a period of around 23 hours, affecting over 25 million customers**[45].

   O2 had significant reliance on Ericsson, the vendor of their mobile network core. O2 **did not have the capabilities in-house** to resolve this issue independently. While Ofcom has made it clear that "outsourcing elements of a network to a third party does not excuse a network provider from its obligations", and that Ofcom "expect all providers to reflect on the steps they are taking […] particularly where reliance is placed on third party suppliers", this is an opportunity for the committee to take this further.

   Our fixed and mobile telecommunications networks are critical national infrastructure. Covid-19 has shown just how critical they are. Therefore, it is a matter of strategic importance to ensure we have the **on-shore capabilities** to **build, maintain, operate, and innovate**, on our **own mobile networks**. The UK has a long and proud history of innovations in telecoms, and there is a clear opportunity to export this knowledge and expertise to our allies and friends around the world. We should work collaboratively with them to ensure we have a **diverse and competitive marketplace for supply of equipment, with diverse and flexible supply chains** – centralised dependency, as we are seeing in some areas due to Covid-19, is **a strategic weakness the UK and allies need to address urgently**.

[45] https://www.ofcom.org.uk/__data/assets/pdf_file/0014/175010/o2-network-outage-cceb.pdf

2. **Encouraging and supporting innovation** in new telecoms networks and services

To grow and maintain industrial capability in this area, it will be necessary for such businesses to be able to **gain domestic revenue and market-share**. Entering an existing market as a new entrant is a challenge, especially given the current limited choice and lack of competition, combined with lack of vendor lock-in and lack of interoperability. But since the UK **does not currently have significant industrial capability in this area** (i.e. it has no design or manufacturing company specialising in 3GPP mobile radio technology), it will **need to be grown**. It is also unlikely that the UK can compete purely on price – with high costs and standards of living, compared with existing vendors which have outsourced their R&D capabilities[46]. Despite this, **it is clearly of strategic importance for the UK to have sufficient domestic, internal capabilities to operate, innovate, and maintain its own telecoms networks**. As these networks become increasingly complex (with the evolution of 5G), and critical to our way of life, it is unthinkable that we do not develop and grow our own domestic capabilities in this field.

3. Creating an environment in the UK where the **incentive structure around investment** in mobile infrastructure is addressed, to facilitate **more secure alternatives**.

A purely profit-focused and revenue-focused approach to building mobile networks will, absent direct and specific enforced regulation, always result in a drive to the **cheapest infrastructure option** – this maximises the potential for profit. DCMS has identified that there is a lack of commercial drivers to improving security in telecoms, as "consumers of telecoms services do not tend to place a high value on security compared to other factors such as cost and quality"[47]. Government's HCSEC monitoring centre has highlighted the issues of systemic poor software development practices. **Security comes at a cost**, and absent Government intervention, will **not be present in the cheapest** available option.

One reason for this is because security aspects are inherently hidden from view – even outside of telecoms, **users generally cannot see the security of the underlying infrastructure**. This means it is not a competitive driver, as users are not able to see the difference between a cheaper operator (using high-risk vendor equipment) and a more expensive operator (perhaps using more expensive European or American equipment that has had extra money spent on security during development).

If the UK's cyber capability is considered akin to how growing of traditional military capability is viewed, then there are important lessons which can be learned from the previous experience in the sourcing, procurement and production of military hardware. For example, the British Nimrod maritime patrol aircraft replacement programme ran over budget by £800m (as many weapons systems programs do), then cost a further £200m to cancel. Between this occurring in 2010 and roll out of the new Poseidon aircraft in 2020, the UK had to borrow aircraft from allies including the US, Germany, France, Norway, and Canada.[48] The important difference **is if a 5G network is compromised due to working with Huawei, a network cannot be borrowed from allies**.

---

[46] https://berthub.eu/articles/posts/5g-elephant-in-the-room/

[47] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

[48] https://www.independent.co.uk/news/uk/home-news/uk-russia-submarines-patrol-planes-nimrod-poseidon-p8-nato-monitor-activity-navy-air-force-security-a8151931.html

Thorsten Benner, director of the Global Public Policy Institute, believes makes UK vulnerable to espionage, sabotage, and blackmail[49]. Blackmail in the arms trade is often referred to as "dependency", where overreliance on a single or a few suppliers can lead to the exporter attempting to exert influence over importers to receive maintenance/spare parts/ordnance. As a major arms supplier, the UK is traditionally in position to exert leverage, not be subject to it – a potential major role reversal.

A German security briefing believes they should avoid "monocultures" by relying on one or few suppliers, others recommend that Germany/EU should develop companies to build a 5G system that is internationally marketable[50]. This is broadly in line with the UK's own objectives around diversifying the supply chain, but the current Government strategy does not appear to enable this, or recognise the issues of allowing approving the involvement of a heavily[51] state-supported[52] international provider to participate as a provider, while simultaneously expecting new entrants to emerge.

There is clearly opportunity for the UK to partner with willing allies around diversification of the supply chain, with aligned interests, but care should be taken to ensure that the UK would itself be able to export and sell this technology on an international stage, along with its allies, rather than merely be a passive participant unable to exploit the work – this is a concern often seen in defence projects, where vetoes on export rights are held by multiple countries involved in R&D and component provision.

17 April 2020

[49] https://foreignpolicy.com/2020/01/31/boris-johnson-britain-knows-its-selling-out-its-national-security-to-huawei/

[50] Germany's CDU stops short of Huawei ban in 5G rollout. February 2020. https://www.ft.com/content/e17ba42a-4ce1-11ea-95a0-43d18ec715f5

[51] https://www.wsj.com/articles/how-the-journal-calculated-huaweis-state-support-11577280830

[52] Huawei looks to state-backed vendor financing. April 2009, https://www.ft.com/content/3f1fd67e-2f56-11de-a8f6-00144feabdc0